CLAIMS

What is claimed is:

1. A method facilitating classification of data flows, comprising

monitoring a data flow associated with a host relative to at least one behavioral attribute;

comparing the at least one behavioral attribute observed in the monitoring step to a knowledge base of at least one known application behavior pattern; and

classifying the data flow based on the comparing step.

2. The method of claim 1 wherein the at least one behavioral attribute is packet size.

3. The method of claim 1 wherein the at least one behavioral attribute is packet size of the first packet in the data flow.

4. The method of claim 1 wherein the at least one behavioral attribute is packet size of the second packet in the data flow.

5. The method of claim 1 wherein the at least one behavioral attribute is packet size of plurality of packets in the data flow.

6. The method of claim 1 wherein the at least one behavioral attribute is the information density associated with at least one packet in the data flow.

7. The method of claim 1 wherein the at least one behavioral attribute is the information density associated with the first packet in the data flow.

8. The method of claim 1 wherein the at least one behavioral attribute is the timing of the data flow relative to at least one similar data flow associated with the host.

9. The method of claim 1 wherein the at least one behavioral attribute is the number of related data flows associated with the host.

10. The method of claim 1 wherein the at least one behavioral attribute is the timing between at least two packets in the data flow.

11. The method of claim 1 wherein the at least one behavioral attribute is a sequence of protocol flags contained in packets of the data flow.

12. The method of claim 1 wherein the at least one behavioral attribute is timing of protocol flags contained in packets of the data flow.

13. The method of claim 1 wherein the at least one behavioral attribute is the timing and sequence protocol flags contained in packets of the data flow.

14. The method of claim 1 wherein the application behavior pattern comprises at least one instance of any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows.

15. The method of claim 1 wherein the application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class.

16. The method of claim 14 wherein the application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class, and wherein the first group of packets are characterized in relation to at least one instance of any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows.

17. A method facilitating classification of data flows, comprising

modeling the behavior of a network application to generate an application behavior pattern; and

configuring a network traffic monitoring device to classify data flows against the application behavior pattern;

wherein the application behavior pattern comprises at least one instance of any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows.

18. The method of claim 17 wherein the application behavior pattern comprises at least one instance of any one of the following: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence of protocol flags, an inter-packet protocol flag timing value.

19. The method of claim 18 wherein the protocol flags are TCP protocol flags.

20. A method facilitating classification of data flows, comprising

monitoring the data flows associated with a host relative to at least one application behavior model corresponding to a traffic class;

matching at least one of the data flows associated with the host to a traffic class, if a threshold number of the data flows match a corresponding application behavior model.

21. An apparatus comprising

a packet processor operative to

detect data flows in network traffic traversing a communications path, the data flows each comprising at least one packet;

parse at least one packet associated with a data flow into a flow specification,

a traffic classification engine operative to

match the data flow to a plurality of traffic classes, at least one of the traffic classes defined by one or more application behavior patterns;

having found a matching traffic class in the matching step, associate the flow specification corresponding to the data flow with a traffic class from the plurality of traffic classes.

22. The apparatus of claim 21 wherein at least one of the plurality of traffic classes is defined by one or more matching attributes, wherein said matching attributes are explicitly presented in the packets associated with the data flows.

23. The apparatus of claim 21 wherein said flow specification contains at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application-specific attribute.

24. The apparatus of claim 22 wherein said flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application-specific attribute.

25. The apparatus of claim 21 further comprising

a flow control module operative to apply bandwidth utilization controls to the data flows based on the traffic class associated with the data flows.

26. A method facilitating classification of data flows, comprising

detecting a data flow in network traffic traversing a communications path, the data flows each comprising at least one packet;

parsing explicit attributes at least one packet associated with the data flow into a flow specification,

matching the flow specification to a first plurality of traffic classes, wherein the first plurality of traffic classes are each defined by one or more matching attributes,

having found a matching traffic class in the matching step, associating the flow specification corresponding to the data flow with a traffic class from the first plurality of traffic classes,

not having found a matching traffic class in the first plurality of traffic classes, matching the data flow to at least one additional traffic class, the additional traffic class defined by an application behavior pattern, the application behavior pattern comprising comprises at least one instance of: a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows.

27. The method of claim 26 wherein the flow specification contains at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application-specific attribute.

28. The method of claim 26 wherein said flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation, a direction of packet flow designation, a protocol type designation, a pair of hosts, a pair of ports, a pointer to a MIME type, and a pointer to an application-specific attribute.

29. A method facilitating the classification of network traffic, comprising

detecting a data flow in network traffic traversing a communications path, the data flow comprising at least one packet;

applying a mathematical function to at least one packet in the data flow to derive a computed value;

comparing the computed value to at least one traffic class, said traffic class defined, at least in part, by a required computed value.

30. The method of claim 29 wherein the required computed value is determined by applying the mathematical function to data flows known to be of the traffic class.

31. The method of claim 29 wherein the mathematical function computes a value indicating the information density of at least one packet.

32. The method of claim 29 wherein the required computed value is a range of values.

33. A method facilitating the classification of network traffic, comprising

detecting a data flow in network traffic traversing a communications path, the data flow comprising at least one packet;

applying a mathematical function to at least one packet in the data flow to derive a checksum;

comparing the computed checksum to the checksum value contained in the at least one packet;

matching the data flow to a traffic class, wherein the traffic class is defined at least in part by whether the computed checksum should match the checksum value in the at least one packet.